V

UNITED STATES DISTRICT COURT

DISTRICT OF DELAWARE

CERTIFIED COPY

SRI INTERNATIONAL, INC.,
a California corporation

Plaintiff and
Counterclaim-Defendant,

vs.

Case No. 04-1199 (SLR)

INTERNET SECURITY SYSTEMS, INC.,
a Delaware corporation; INTERNET
SECURITY SYSTEMS, INC., a Georgia
corporation; and SYMANTEC
CORPORATION, a Delaware corporation,

Defendants and
Counterclaim-Plaintiffs.
_______________________________________/

DEPOSITION OF GEORGE KESIDIS
VOLUME I

DATE: May 25, 2006

TIME: 9:13 a.m.

LOCATION: DAY CASEBEER MADRID &
BATCHELDER
20300 Stevens Creek Boulevard
Suite 400
Cupertino, CA 95014

REPORTED BY: KAREN L. BUCHANAN
CSR No. 10772

8696
21416

Bell & Myers
CERTIFIED SHORTHAND REPORTER, INC.

50 AIRPORT PARKWAY, SUITE 205, SAN JOSE, CALIFORNIA 95110, TELEPHONE (408) 287-7500, FAX (408) 294-1211

reacts to route updates and other kinds of 10:32:13
OSPF-related messages that are delivered by packets. 10:32:16
So I can't say that it doesn't react to packets, 10:32:20
therefore. 10:32:26

Q. So is it your opinion that algorithms that 10:32:31
look at information about routing would not be 10:32:39
relevant to the patents in suit? 10:32:40

MR. POLLACK: Objection. Lacks foundation, 10:32:43
vague and ambiguous. 10:32:47

THE WITNESS: I would say no. I would say 10:32:52
that it depends on how you look at those packets. And 10:32:56
that's the key difference between a host-based and a 10:32:59
network-based sensor. It's really a matter of the -- 10:33:05
how you react to them and the kinds of -- the kinds of 10:33:11
operations you do as a result of observing such a 10:33:14
packet and how you observe the packet: Are you simply 10:33:19
taking note of the fact that it's a packet, or are you 10:33:24
probing deeper into the payload, and everything in 10:33:27
between. It's really fundamentally a question 10:33:34
about -- I think I said, how you're reacting to the 10:33:38
packet and what attributes of the packet you're 10:33:42
reacting to. 10:33:42

BY MS. MOEHLMAN: 10:33:56

Q. What attribute -- if you were looking at a 10:33:59
routing protocol, what attributes of a routing

protocol would you have to look at in order to be relevant to the patents in suit? 10:34:06 10:34:07

MR. POLLACK: Objection. Vague and ambiguous, incomplete hypothetical. 10:34:12 10:34:14

THE WITNESS: So if, for example, you -- you were to examine routing packets in a network service monitor, according to the packets in suit, you may be using those -- you may be taking stock of rather gross statistics, the total number, say, of packets, irrespective of where they're going or coming from. You could be looking at compiling statistics based on other -- let's see. I'm just trying to think. I mean in terms of how you might do protocol anomaly detection in a network intrusion detection monitor versus protocol anomaly detection JiNao style, the former is a significantly more primitive kind of pad using far less information about the substance of the packet, what's in the packet, and a much more rudimentary model of the protocol itself in order to conduct protocol anomaly analysis. 10:34:25 10:34:36 10:34:41 10:34:51 10:34:57 10:35:03 10:35:13 10:35:17 10:35:20 10:35:27 10:35:29 10:35:34 10:35:38 10:35:46 10:35:54 10:35:54

BY MS. MOEHLMAN: 10:36:03

Q. Go ahead. 10:36:04

A. I'm not sure I answered your question precisely. 10:36:06 10:36:12

Q. If you could take a look at Kesidis

Exhibit 4, which is the '338 patent, if you take a 10:36:18
look at claim 1 of that patent. 10:36:20

A. Sure. 10:36:20

Q. Can you show me exactly where claim 1 10:36:24
indicates that the rudimentary model used by JiNao is 10:36:31
different somehow from what's in this claim? 10:36:33

MR. POLLACK: Objection. Vague and 10:36:35
ambiguous, lacks foundation, mischaracterizes the 10:36:36
testimony. 10:36:39

THE WITNESS: Okay. I'll give it a try. The 10:36:46
key thing to my mind is the -- that it's a method of 10:37:00
network surveillance. And so you're, in this context, 10:37:03
looking at all the packets on the wire, not just those 10:37:13
that are being sent to a particular router. 10:37:23

So the fundamental difference is that the 10:37:26
network entity or the network -- method of network 10:37:31
surveillance, you don't have a lot of information 10:37:33
about how the actual protocol itself is functioning 10:37:38
inside the router. That information is not known to 10:37:42
the network service entity, network service monitor. 10:37:51

So in my opinion, you don't have the basis to 10:37:55
do the kind of detailed per-host or per-router 10:38:02
protocol anomaly detection in this context just based 10:38:05
on the preamble that you would in a JiNao context 10:38:11
where I'm essentially sitting inside a router, just

one router, and trying to evaluate the anomalies of 10:38:19
the protocol that it's participating in. 10:38:19

MS. MOEHLMAN: 10:38:22

Q. Is a router a network entity? 10:38:24

A. A router -- sure. It's an entity in an 10:38:34
absolute sense, but in the context of this claim, I 10:38:48
think you -- your method is being conducted outside of 10:38:52
the router without the benefit of knowledge of its 10:38:57
internal machinations. And so you're -- you may, for 10:39:09
example, be tapping into the -- a link that is 10:39:20
connected to a router, and so therefore, the packets 10:39:23
that are flowing through it, of course, are handled by 10:39:26
the network entity. 10:39:31

So sorry, your question was is it a network 10:39:35
entity, and I would say yes, it's a network entity. 10:39:37

Q. Please define what you understand to mean by 10:39:40
network surveillance. 10:39:41

A. Well, there, you're examining the packets on 10:39:47
the wire. 10:39:53

Q. What are you examining about the packets on 10:39:55
the wire? Are you examining every particular field 10:39:59
of a packet on a wire? What exactly do you need to 10:40:03
examine about a packet on a wire? 10:40:06

MR. POLLACK: Objection. Vague and 10:40:08
ambiguous.

MS. MOEHLMAN: I'm just trying to understand your testimony, because you just spent several pages talking about how the network packets examined by JiNao don't fall within this claim. And you pointed to network surveillance. So when I asked you about network surveillance, you testified that you look at all packets on the wire. So when you say all packets on the wire, what particularly do you need to look at within a packet, or could it be anything? 10:40:10 10:40:14 10:40:18 10:40:22 10:40:25 10:40:28 10:40:31 10:40:35 10:40:37

MR. POLLACK: Objection. Mischaracterizes the testimony. Vague and ambiguous. Lacks foundation. 10:40:39 10:40:43 10:40:49

THE WITNESS: So the point is that when I have -- when I'm doing network surveillance, I'm looking at the packets as they're flowing by on the wire or through some reconnaissance port of the router. And all I have to -- in the sense of just trying to deal with this torrent of information, I'm typically, in the cont,ext of these patents examining fields in the header of the packet. And only in a very, very rudimentary way could I be exploring elements of the payload. 10:40:51 10:40:54 10:40:57 10:41:04 10:41:10 10:41:14 10:41:18 10:41:27 10:41:31 10:41:31

BY MS. MOEHLMAN: 10:41:36

Q. And how did JiNao not look at packets flowing on the wire? 10:41:39

A. Well, in a couple of ways. The first is that 10:41:51
it's examining only those packets that are in receipt 10:41:58
by the router that it's trying to protect and on which 10:42:04
it's trying to conduct intrusion detection. And only 10:42:12
those packets that, in the case of the example in the 10:42:15
paper, are germane to OSPF. And it's certainly 10:42:29
reacting to elements in the payload to a level of 10:42:31
detail that's simply out of the scope of these patents 10:42:34
and would simply not be feasible. I went through the 10:42:43
noninfringement story with regards -- sorry, the 10:42:47
validity story with regard to JiNao in my report, and 10:42:51
I could look through it. 10:42:53

Q. Feel free to reference it if you need to. 10:42:55
But I'm trying to ask you questions, and if you need 10:42:59
to reference it, that's why I marked all of these 10:43:03
exhibits, so feel free. Let me ask you, just going 10:43:10
to the next element on the '338 patent where it says, 10:43:15
"receiving network packets handled by a network 10:43:18
entity." I believe you said a router is a network 10:43:25
entity. Am I right? 10:43:25

A. Sure. 10:43:27

Q. And did JiNao receive packets handled by a 10:43:32
router? 10:43:39

MR. POLLACK: Objection. Vague and 10:43:39
ambiguous.

THE WITNESS: In that context, sure. It 10:43:44
reacted to packets that are -- certain packets that 10:43:47
are received by the router. So in the sense that it 10:43:56
reacts to those packets, it receives them. 10:43:56

BY MS. MOEHLMAN: 10:44:11

Q. And as part of the OSPF protocol, is there 10:44:17
something called a HELLO packet? 10:44:19

A. Sure. 10:44:20

Q. And what does a HELLO packet do? 10:44:23

A. It simply identifies the OSPF speaker to its 10:44:32
peers. 10:44:41

Q. And does that indicate a network connection? 10:44:45

MR. POLLACK: Objection. Vague and 10:44:46
ambiguous. 10:44:46

THE WITNESS: Network connection? In a very 10:44:54
general sense, yes. Essentially, if I'm in receipt of 10:45:06
a HELLO packet from an OSPF speaker, I know that that 10:45:10
speaker is therefore connected to the network. 10:45:10

BY MS. MOEHLMAN: 10:45:12

Q. Did JiNao build long-term profiles, 10:45:19
long-term statistical profiles? 10:45:21

MR. POLLACK: Objection. Vague and 10:45:25
ambiguous. 10:45:26

THE WITNESS: Well, I guess in my reading of 10:45:29
JiNao, I can't really say that it -- you know, in my

reading of JiNao, I can't really say that it built 10:45:40
long-term profiles in the same fashion and using the 10:45:47
same event stream, if we want to call it that, drawing 10:45:51
language from the patent claim, that the patent did. 10:45:57

A good way to think of it is that it didn't 10:46:01
represent those long-term profiles -- sorry, it didn't 10:46:06
represent -- if it did have a sense of baseline 10:46:14
activity, nominal baseline activity of the protocol 10:46:18
that it's trying to protect, it certainly doesn't 10:46:20
represent that baseline activity as a long-term 10:46:24
statistical profile in the manner of the patents. 10:46:24

BY MS. MOEHLMAN: 10:46:29

Q. Is it your testimony -- putting aside the 10:46:33
patents for a second, is it your testimony or your 10:46:36
opinion that JiNao didn't build long-term statistical 10:46:42
profiles -- 10:46:42

MR. POLLACK: Objection. 10:46:42

BY MS. MOEHLMAN: 10:46:44

Q. -- as you understand the term "statistical 10:46:46
profile"? 10:46:47

MR. POLLACK: Objection. Vague and 10:46:48
ambiguous. Lacks context. 10:46:49

THE WITNESS: I think that the answer to that 10:46:50
question as you've asked it is yes, that JiNao does 10:46:54
build long-term profiles.

BY MS. MOEHLMAN: 10:46:56
Q. Does JiNao build short-term profiles? 10:47:00
MR. POLLACK: Same objections. 10:47:01
THE WITNESS: I wouldn't say that it builds 10:47:06
short-term profiles anything like the -- the -- 10:47:12
anything like the network service monitor of the 10:47:16
patents would. 10:47:16
BY MS. MOEHLMAN: 10:47:17
Q. I'm just asking you, did it build something 10:47:21
that, just using the definition that you understand 10:47:25
short-term profile to mean, separate and apart from 10:47:29
the particular data stream described in the patent? 10:47:33
A. I see. I see the question you're asking. 10:47:35
MR. POLLACK: Objection. Lacks foundation. 10:47:39
Vague and ambiguous. 10:47:40
THE WITNESS: You know, JiNao does leverage a 10:47:43
lot of the ideas of IDES. And the answer to your 10:47:47
question as it's phrased is yes. 10:47:47
BY MS. MOEHLMAN: 10:47:52
Q. Does JiNao compare a long-term statistical 10:47:58
profile and a short-term statistical profile? 10:48:01
MR. POLLACK: Same objections. 10:48:02
THE WITNESS: You know, in the context, in 10:48:04
the way that IDES does, yes. 10:48:04
MS. MOEHLMAN:

BY MS. MOEHLMAN: 10:46:56

Q. Does JiNao build short-term profiles? 10:47:00

MR. POLLACK: Same objections. 10:47:01

THE WITNESS: I wouldn't say that it builds short-term profiles anything like the -- the -- anything like the network service monitor of the patents would. 10:47:06 10:47:12 10:47:16 10:47:16

BY MS. MOEHLMAN: 10:47:17

Q. I'm just asking you, did it build something that, just using the definition that you understand short-term profile to mean, separate and apart from the particular data stream described in the patent? 10:47:21 10:47:25 10:47:29 10:47:33

A. I see. I see the question you're asking. 10:47:35

MR. POLLACK: Objection. Lacks foundation. Vague and ambiguous. 10:47:39 10:47:40

THE WITNESS: You know, JiNao does leverage a lot of the ideas of IDES. And the answer to your question as it's phrased is yes. 10:47:43 10:47:47 10:47:47

BY MS. MOEHLMAN: 10:47:52

Q. Does JiNao compare a long-term statistical profile and a short-term statistical profile? 10:47:58 10:48:01

MR. POLLACK: Same objections. 10:48:02

THE WITNESS: You know, in the context, in the way that IDES does, yes. 10:48:04 10:48:04

MS. MOEHLMAN:

Q. Does JiNao have a mechanism to determine whether the difference between the short-term profile and the long-term profile indicates a significant difference, if there is a significant difference, between the long-term and short-term profile? 10:48:12 10:48:15 10:48:21 10:48:23 10:48:28

MR. POLLACK: Objection. Vague and ambiguous. 10:48:28 10:48:29

THE WITNESS: Most of your question -- what do you mean by a "mechanism"? 10:48:30 10:48:30

BY MS. MOEHLMAN: 10:48:33

Q. Does JiNao use the NIDES, IDES algorithm to determine whether there is a difference -- 10:48:37 10:48:40

A. A statistically significant difference? Is that what you're trying to say? 10:48:43 10:48:45

Q. Yes. 10:48:45

A. Yes, in that sense, it does. 10:48:49

Q. So, now, going back to claim 1 of the '338 patent, do you believe that JiNao received network packets handled by a network entity? 10:48:53 10:48:58 10:49:03

A. In the sense that it reacts to them, yes. Certain packets. 10:49:10 10:49:12

Q. Do you believe that it meets the claim limitation recited in claim 1? 10:49:16 10:49:18

A. No, I don't. 10:49:18

Q. Why not?

A. Because it's not -- it's fundamentally not a method of network surveillance. 10:49:22 10:49:24

Q. So it's your opinion that it does not meet the preamble? 10:49:27 10:49:29

A. That's correct, yeah. 10:49:38

Q. Does it meet the first element, receiving network packets handled by a network entity? 10:49:42 10:49:47

MR. POLLACK: Objection. Vague and ambiguous. 10:49:48 10:49:48

THE WITNESS: The router receives the packets, strictly speaking. So JiNao is a mechanism sitting in a router that reacts to the receipt of those packets. So I would say qualifying it, yeah, you're right. 10:49:51 10:49:55 10:49:57 10:50:01 10:50:01

BY MS. MOEHLMAN: 10:50:06

Q. So does JiNao meet that first element or not? 10:50:11 10:50:12

A. I -- I mean, again, it's not receiving the network packet. It's reacting to certain attributes of it that are -- the packets already in receipt by the router or the line card on which JiNao is functioning. 10:50:16 10:50:20 10:50:24 10:50:28 10:50:29

Q. So if I had a component that receives data from a router, would that meet the claim? Could that possibly meet that claim element? 10:50:34 10:50:40

MR. POLLACK: Objection. Vague and 10:50:43
ambiguous. 10:50:44

THE WITNESS: If you added a component? Say 10:50:45
that again. I'm sorry. 10:50:45

BY MS. MOEHLMAN: 10:50:46

Q. If I had a component that received, through 10:50:50
the router, network packets, could that meet the 10:50:54
claim -- that first element of claim 1? 10:51:00

A. It's a little bit -- why would you have a 10:51:03
component -- the router's job is to receive and 10:51:07
transmit packets. So you would have to have JiNao -- 10:51:09
what I'm saying is the router receives the packets, 10:51:13
and JiNao -- it unbundles them from the frame. The 10:51:18
network processor examines the header of the packet. 10:51:22

Q. And would that be sufficient to meet the 10:51:25
limitation of receiving network packets handled by a 10:51:27
network entity? 10:51:28

A. You would -- so you're asking if I combine 10:51:33
JiNao with the front end of the ingress line card, 10:51:36
then yes. Then it would be receiving -- the front end 10:51:41
certainly receives. That's its job, to receive 10:51:44
packets. 10:51:50

Q. Now, is it your understanding of the JiNao 10:51:55
paper that it describes the use of a router to 10:51:57
receive network packets?

A. Well, there's -- the majority of the JiNao paper is targeting the OSPF context, the specific example of doing anomaly detection for OSPF. So that is -- the OSPF protocol is executed by routers, interior gateway protocol executed by routers. No other entities in the enterprise would run OSPF but routers. 10:52:04 10:52:09 10:52:17 10:52:22 10:52:28 10:52:31 10:52:32

I'm sorry, let -- can you just rephrase your question? Because maybe I didn't understand it. 10:52:35 10:52:37

Q. I just want to understand if in the JiNao paper that you have reviewed, and the JiNao material, if it's your understanding that JiNao receives packets off the wire or receives packets in connection with a router. 10:52:41 10:52:45 10:52:50 10:52:56 10:52:57

A. Right. Right. So the way I understand the -- I mean there is text in JiNao about generalizing it and applying it to other protocols sometime in the future. The specific example that JiNao -- that JiNao fleshes out in the paper has to do with OSPF, and the idea is that the front end of the router is receiving the packet, unbundling it, deciding that it is, in fact, a router -- it's a packet that contains a routing message and sending it off to the CPU that's executing the protocol, the finite state machine that's executing the OSPF 10:53:00 10:53:02 10:53:05 10:53:09 10:53:15 10:53:19 10:53:23 10:53:27 10:53:33 10:53:37

protocol in the line card. And JiNao is sitting 10:53:43
there, intercepting that packet, that information as 10:53:49
it's in receipt of the finite state machine and 10:53:56
conducting intrusion -- or protocol anomalily 10:53:58
detection. 10:53:59

And I'm still not sure if I answered your 10:54:01
question. So if you want to ask it again, feel free. 10:54:03

Q. And I think that you've testified earlier 10:54:06
that building -- that JiNao builds at least one 10:54:10
long-term and at least -- that JiNao discloses 10:54:13
building at least one long-term and at least one 10:54:18
short-term statistical profile, correct? 10:54:19

A. In the same manner of IDES, I would agree to 10:54:22
that. 10:54:22

Q. And it discloses the use of HELLO packets, 10:54:25
and I believe you testified earlier that HELLO 10:54:28
packets could be considered a measure of network 10:54:31
connections; is that correct? 10:54:32

MR. POLLACK: Objection. Mischaracterizes, 10:54:34
vague and ambiguous, lacks foundation. 10:54:37

THE WITNESS: You know, I did say that, and 10:54:46
I'm not going to refute it. But I'd just say that a 10:54:50
HELLO packet being interpreted as a network connection 10:54:53
is simply not in the spirit of the specification of 10:54:56
the patent.

BY MS. MOEHLMAN: 10:54:58

Q. Does it meet the claim language? 10:55:03

A. Obviously, yeah. 10:55:05

Q. And I believe you also testified that JiNao 10:55:10 discloses comparing at least one long-term and at 10:55:12 least one short-term statistical profile in the 10:55:15 manner of IDES and NIDES, correct? 10:55:17

A. In the manner of IDES and NIDES, yes. 10:55:19

Q. And I believe you also testified that JiNao 10:55:22 discloses determining whether the difference between 10:55:24 the short-term statistical profile and the long-term 10:55:27 statistical profile is statistically significant, 10:55:29 correct? 10:55:30

A. In the manner of IDES and NIDES, yes. 10:55:34

Q. Is it your opinion that statistically 10:55:40 significant differences would indicate suspicious 10:55:44 activity? 10:55:44

MR. POLLACK: Objection. Vague and 10:55:50 ambiguous. 10:55:51

THE WITNESS: Statistically significant 10:55:52 differences in what? 10:55:52

BY MS. MOEHLMAN: 10:55:53

Q. Just in general. 10:55:54

A. No. 10:55:54

Q. What would make a statistically significant

difference between a long-term and a short-term 10:56:00
profile be indicative of suspicious network activity? 10:56:05

MR. POLLACK: Objection. Incomplete 10:56:07
hypothetical, vague and ambiguous, overbroad. 10:56:08

THE WITNESS: Well, I mean if the -- it has 10:56:16
to be -- so you're asking the question if there is a 10:56:21
significant difference, what makes it suspicious? 10:56:21

BY MS. MOEHLMAN: 10:56:25

Q. Yes. 10:56:26

A. I guess the answer to that would be knowledge 10:56:35
of past or, you know, some kind of expertise regarding 10:56:41
that difference being caused by a malicious act or 10:56:44
possibly being caused by a malicious act. 10:56:47

Q. How does the patent disclose determining 10:56:51
whether the difference between a short-term 10:56:55
statistical profile and the long-term statistical 10:56:58
profile indicates suspicious network activity? 10:57:01

MR. POLLACK: Objection. Vague and 10:57:01
ambiguous. 10:57:02

THE WITNESS: How does the patent disclose 10:57:05
determining whether -- it identifies -- to begin with, 10:57:23
it identifies elements, in what I understand is called 10:57:30
the Markush list, data transfer errors and network 10:57:37
connections in the independent claim 1. 10:57:40

So it develops what they call an event

stream. It builds statistics or an event stream based 10:57:54
on packets that belong to those categories. And when 10:57:57
it detects anomalous -- anomalies in those short-term 10:58:03
statistics compared to long-term statistical versions 10:58:06
of the same thing or historical expectations, it 10:58:10
sounds an alert. 10:58:12

So I'm sufficiently vague at this point. But 10:58:15
what -- obviously an error could be caused by 10:58:19
something that is completely legitimate, or an error 10:58:23
could be something that's malicious, that's 10:58:28
maliciously caused. 10:58:30

So to the extent that you have a significant 10:58:34
statistical deviation in the short-term and long-term 10:58:39
versions of the statistics of elements in the Markush 10:58:43
review, you call it, I don't know, you call it a 10:58:47
suspicious event. 10:58:48

So I still haven't said anything about 10:58:50
specifically what that could be, but with regard to 10:58:53
expertise, as to, for example, what a DOS attack or a 10:59:00
worm attack and how it might exhibit behavior in the 10:59:08
statistics you're building, based on the Markush group 10:59:12
here, that's essentially how you decide you're going 10:59:15
to sound an alert. 10:59:16

So there is knowledge of certain kinds of 10:59:20
attacks yield anomalies in -- statistical anomalies in

A. Sure. 11:11:00
Q. It would build a long-term profile, based on 11:11:06
a measure of network connections, correct, that would 11:11:08
be the three; is that correct? 11:11:09
MR. POLLACK: Objection. Vague and 11:11:13
ambiguous. 11:11:13
THE WITNESS: Okay. 11:11:13
BY MS. MOEHLMAN: 11:11:15
Q. Is that correct? I'm trying to understand 11:11:18
your testimony. 11:11:19
A. Well, you're qualifying it a little bit, but 11:11:22
yeah, I mean your connection attempts, but -- yeah. 11:11:27
Q. And you could also look at -- 11:11:35
A. Or you could even refer to it in terms of 11:11:37
errors, if it's an unacknowledged connection attempt. 11:11:40
That could be referred to as an error. It's not a 11:11:44
data transfer, because it's not a data plain story 11:11:46
yet. 11:11:47
Q. And it would be building short-term 11:11:51
profiles, correct, by looking at the same measure, 11:11:55
correct? 11:11:56
MR. POLLACK: Objection. Vague and 11:11:59
ambiguous, mischaracterizes. 11:12:04
THE WITNESS: Right. 11:12:04
BY MS. MOEHLMAN:

Q. Okay. It would compare the baseline of 11:12:09
three with the short-term profile, correct? 11:12:13

A. It would compare the baseline three? 11:12:16

Q. That would be what we called the long-term 11:12:19
profile, right? 11:12:21

A. Again -- 11:12:22

Q. The method you're talking about. 11:12:24

A. In a very rudimentary way. Again, in my 11:12:30
opinion, the example I gave is an extremely 11:12:35
rudimentary example. This is -- 11:12:39

Q. Well, would it meet the element of comparing 11:12:41
at least one long-term and at least one short-term 11:12:46
statistical profile of the '338 patent? 11:12:47

MR. POLLACK: Objection. Vague and 11:12:48
ambiguous. 11:12:49

THE WITNESS: Well, if you kind of remove in 11:12:52
my example the notion of a policy, where I'm simply 11:12:55
calling out an alert by definition, when I see 11:13:04
three -- when the monitor observes three 11:13:08
unacknowledged SYNs, for example, and infers that this 11:13:11
is three failed login attempts to a protected machine, 11:13:16
in a sense, it's not looking for a statistical 11:13:19
anomaly. It's simply called out as a signature of 11:13:22
something that is defined to be an attack. 11:13:27

So, you know, if you want to -- very loosely

interpret that kind of policy as a, you know, 11:13:37
represent it as a long-term statistical profile, I'm 11:13:49
not even clear that it's a long-term statistical 11:13:53
profile. You have -- login attempts may be endemic, 11:13:57
and you may simply call out the fact that three failed 11:14:02
login attempts is the signature of a problem, and I'm 11:14:04
going to alert based on that observance in the short 11:14:07
term. 11:14:07

So I think I -- I think the stretch here is 11:14:14
in -- in the signature-based approach is looking at 11:14:17
the long-term profile and identifying something that 11:14:20
is short of the signature, anything short of the 11:14:24
signature as being a long-term profile. And that's 11:14:27
what I have trouble identifying. 11:14:27

MS. MOEHLMAN: 11:14:28

Q. So is it your opinion that your example 11:14:32
would meet claim 1 of the '338 patent or would not 11:14:35
meet claim 1? 11:14:36

A. I guess what I was trying to do is make it 11:14:38
meet claim 1 and I failed. I don't even think the 11:14:42
rudimentary example of three failed login attempts. 11:14:45

Q. So that does not meet claim 1 in your 11:14:48
opinion? 11:14:48

A. I don't think it meets claim 1. 11:14:50

Q. And why, in your opinion, does it not meet claim 1? Which elements are not -- 11:14:55

A. Because the lack -- not quite meeting a long-term profile is not really what the -- sorry, not quite meeting a signature, if a short-term profile doesn't quite meet the conditions of a signature, then that notion of not quite meeting the conditions of a deterministic signature is not interpretable as a long-term profile. 11:14:59 11:15:05 11:15:08 11:15:12 11:15:16 11:15:21 11:15:22

Just -- in other words, what we're trying to say is can we make "just shy of a signature" mean a long-term statistical profile or even a long-term statistical baseline plus a deviated -- like an expected standard deviation or multiple standard deviations. 11:15:24 11:15:28 11:15:32 11:15:38 11:15:44 11:15:44

And that's what you're missing when you're trying to detect a signature. Just shy of three failed login attempts is not a long-term statistical profile baseline plus standard deviation, if that's our -- or multiple standard deviations. 11:15:46 11:15:53 11:15:53 11:15:53 11:16:01

(Reporter interruption.) 11:16:01

THE WITNESS: In the example, if my short-term profile or if my signature is three failed login attempts over, say, a time window, then it doesn't trip if I'm -- my alert doesn't trip if I'm just shy of that. And "just shy of that" does not 11:16:04 11:16:07 11:16:10 11:16:14

satisfy my understanding of what long-term statistical 11:16:24
profile is. 11:16:24

BY MS. MOEHLMAN: 11:16:24

Q. What is your understanding of what long-term 11:16:27
statistical profile is? 11:16:28

A. Well, it's a measure of nominal baseline 11:16:32
activity, first. It's a nominal baseline activity, 11:16:36
innocuous activity with respect to the specific stat 11:16:49
you're looking at, statistics you're computing for a 11:16:56
particular instance of the element of the Markush 11:16:59
group. So you have a short-term statistic that you're 11:17:04
computing in real-time, and you have a baseline for 11:17:07
it, the long-term statistics. And when there is 11:17:12
significant statistical deviation between the two, 11:17:16
positive or negative, up or down, you call it an 11:17:19
alert. 11:17:20

Q. And because you're looking for -- well, what 11:17:23
is significant? 11:17:26

A. Again, there is a certain -- this has to do 11:17:37
with what is -- the question you're asking is what is 11:17:39
the standard deviation of your short-term profile. 11:17:42

You have a long-term baseline, which is 11:17:50
saying you expect -- for example, just give a concrete 11:17:55
example. Say you expect 10 percent of the packets you 11:17:58
observe over a sliding packet window to have a certain

property, and you've observed your system under 11:18:04
nominal conditions, and you note that that 10 percent 11:18:07
is a nominal amount to expect, and you conduct a -- 11:18:14
you're calculating a short-term profile at any given 11:18:17
point in time in your monitor, and you observe that 11:18:21
your short-term profile is at 20 percent. Now, is the 11:18:32
difference statistically significant? 11:18:34

And the answer to that question is it 11:18:36
depends. It depends on the variance of your estimate 11:18:40
in your short-term profile. So your long-term 11:18:45
profile, even though you're averaging over a time 11:18:48
window or packet count, is nevertheless a random 11:18:53
variable. It's nevertheless changing. It's 11:18:55
oscillating. 11:18:55

So if you -- say if I exceed the baseline 11:19:00
value of 10 percent just once, I may call it an alert, 11:19:03
but it may be a false positive, because I have a 11:19:08
certain variance in that estimate. 11:19:09

And so this is where you want to have rules 11:19:13
of thumb or such as three standard deviations. So I 11:19:17
estimate not only the mean, but I ought to estimate 11:19:19
the standard deviation in the usual way, the typical 11:19:22
way. And I look for three or two standard deviations 11:19:27
away from the baseline. 11:19:28

So if my current estimate -- say I'm looking

to exceed the baseline. If my current estimate minus 11:19:36
two sample standard deviations are greater than the 11:19:41
baseline value, then I sound an alert. 11:19:48

And even in the learning of that difference, 11:19:54
the learning or the stipulation of that difference, 11:20:02
there are rules of thumb. So in a sense, it's a 11:20:12
question of how much tolerance you want. And that 11:20:17
often is informed by knowledge of the innocuous 11:20:20
traffic, as well. 11:20:21

So when you're taking your long-term profile, 11:20:23
again in the usual way, you may observe variance in 11:20:28
your innocuous long-term profile. So there is 11:20:31
variance in your short-term, there is variance in your 11:20:34
long-term, and you take stock of both when you're 11:20:36
trying to figure the difference between the two that 11:20:39
should trigger an alert. 11:20:40

Q. So when I read the claim limitation, 11:20:44
determining whether the difference between the 11:20:45
short-term statistical profile and the long-term 11:20:48
statistical profile -- I'm sorry, so let me not say 11:20:54
"me," because I'm not a person of skill in the art. 11:20:56
When a person of skill in the art is reading the 11:21:01
determination whether the difference between the 11:21:03
short-term statistical profile and the long-term 11:21:05
statistical profile indicates suspicious network

enabled, right? 14:03:56

A. That's right. That's the opinion I offered, 14:03:58
right. 14:03:58

Q. So I take it that given your testimony, 14:04:03
you're not relying on the code in the appendix for 14:04:06
your opinion regarding enablement? 14:04:13

A. Well, like I said, I'm not sure what the 14:04:18
relationship is between the code in the appendix and 14:04:21
what was escrowed. I just don't know. I mean I don't 14:04:24
know that it's -- what was escrowed was a subset or a 14:04:31
modification or -- what was escrowed was a superset or 14:04:35
a modification of what was submitted as an appendix to 14:04:38
the patents. 14:04:38

Q. Are you relying on any SRI source code in 14:04:42
your enablement arguments? 14:04:47

A. Beyond simply saying that I looked at the 14:04:52
source code and other EMERALD-related documents and 14:04:55
made the statement that I think they implement the 14:05:00
claims, beyond that -- I'm sorry, can you rephrase the 14:05:06
question? 14:05:06

Q. Do you believe that the patent specification 14:05:15
enables the claims of the patents in suit? 14:05:17

A. The patent specification enables the claims 14:05:20
of the patents in suit? Let's see. Yes, I believe 14:05:23
the patent spec enables the claims.

Q. Do you rely on any code that's in the 14:05:31
appendix for that opinion? 14:05:39

A. I guess I'm not sure that I do, because the 14:05:44
code I looked at, I'm not sure if it was what was 14:05:49
actually in the appendix or -- so I don't -- I simply 14:05:53
don't know if what was escrowed to me is what was 14:05:56
appended to the patents when they were filed. So I 14:05:59
don't know how to answer that question. 14:06:01

Q. What material are you relying on for your 14:06:04
opinion that the claims of the patents in suit are 14:06:08
enabled? 14:06:08

A. The claims -- enabled by what? 14:06:11

Q. You set forth an opinion, did you not, 14:06:11
that -- 14:06:14

A. By EMERALD? 14:06:16

Q. -- that the patents in suit -- do you 14:06:19
understand what enablement is, Dr. Kesidis? 14:06:23

A. Sure. 14:06:23

Q. What is enablement? 14:06:25

A. Enablement means they're functioning in an 14:06:29
implementation of the claims, that perform what's set 14:06:37
out in the claims. You give enough of a disclosure 14:06:41
that so someone of ordinary skill can build such -- 14:06:45
can build such a functioning implementation of what's 14:06:51
stated in the claims.

Q. And in forming your opinions on enablement, do you rely on anything other than the figures and the text of the patent specification? 14:06:58 14:07:02 14:07:09

A. Yes. Well, insofar -- I can say yes, because I make reference -- I make -- pardon me a second. I make reference to -- for example, in my statement of EMERALD's embodiment of claim '615, I make reference to mCorr, for example, which I'm reasonably sure -- as I understand it, reasonably sure was not disclosed in the appendix. Again, I'm not a hundred-percent sure. I did look at the code in what was escrowed, so I have to say that I am relying on material that was escrowed here to claim that EMERALD is an embodiment of the claims. 14:07:21 14:07:50 14:07:54 14:08:00 14:08:04 14:08:08 14:08:16 14:08:22 14:08:29 14:08:33 14:08:33

Q. What I'm talking about -- if you take out Kesidis Exhibit 3, which is your rebuttal report on validity. 14:08:38 14:08:43 14:08:44

A. Right. 14:08:44

Q. And if you turn to page 7 of that report, there is a section entitled "Enablement." 14:08:47 14:08:50

A. Right. 14:08:51

Q. And you state: 14:08:52

"I have reviewed the patent specification and claims. While not reciting every detail of a fully 14:08:54 14:09:00

implemented product, the patent 14:09:03
specifications do provide sufficient 14:09:05
information to teach one of ordinary 14:09:07
skill in the art how to practice the 14:09:09
claimed inventions without undue 14:09:12
experimentation." 14:09:13

A. Okay. 14:09:14

Q. Do you understand what enablement is? 14:09:16

A. Sure. In that sense. 14:09:17

Q. What is enablement? 14:09:20

A. Again, is there a disclosure in the patent spec that would describe to one of ordinary skill how to develop an implementation of what's described in the claims without undue experimentation. 14:09:24 14:09:27 14:09:44 14:09:44

Q. In order to form your opinion on enablement in this section, do you rely on any SRI source code? 14:09:44 14:09:45

MR. POLLACK: Objection. Vague and ambiguous. 14:09:50 14:09:50

THE WITNESS: In this particular context, I was primarily looking at the patent spec and asking myself a question as to whether the particular implementation that's described in the preferred embodiment teaches one of ordinary skill how to implement the claims. 14:09:52 14:09:58 14:10:02 14:10:05 14:10:10 14:10:10

BY MS. MOEHLMAN:

Q. Do you rely on any of the source code in the 14:10:15
appendix to form your opinion on enablement? 14:10:19

MR. POLLACK: Objection. Asked and answered, 14:10:22
vague and ambiguous. 14:10:22

THE WITNESS: In this particular context, I'm 14:10:25
not. 14:10:25

BY MS. MOEHLMAN: 14:10:26

Q. Do you rely on any incorporated reference in 14:10:31
the patent specification in order to have your -- to 14:10:35
form your opinion on enablement? Let me restate 14:10:35
that. 14:10:39

Did you rely on any incorporated reference in 14:10:42
the patent specification in forming your opinion on 14:10:46
enablement? 14:10:47

MR. POLLACK: Objection. Vague and 14:10:48
ambiguous, lacks foundation. 14:10:55

THE WITNESS: You're referring to the 14:11:00
referred prior publications and patents -- 14:11:00

BY MS. MOEHLMAN: 14:11:02

Q. I'm referring to anything in the text -- 14:11:08

A. -- by disclosed reference. 14:11:10

Q. I'm referring to anything in the text, just 14:11:12
the text, not in the list of other publications or 14:11:16
patents, but in the actual written text of the 14:11:16
patent.

A. If I look at the written text -- 14:11:22

MR. POLLACK: Hang on a second. Objection. 14:11:25
Vague and ambiguous, clearly lacks foundation. I 14:11:28
think it's obvious the witness doesn't know what 14:11:30
you're asking. 14:11:31

THE WITNESS: If you're asking if based on 14:11:34
the patent specification, if I believe the patent 14:11:39
specification enables the claims, that's what I was 14:11:41
trying to get across in section 7 of this rebuttal 14:11:46
report. 14:11:46

MS. MOEHLMAN: 14:11:47

Q. In reviewing patent specification, did you 14:11:50
come across any papers that were incorporated by 14:11:54
reference? 14:11:54

MR. POLLACK: Objection. Lacks foundation, 14:11:56
vague and ambiguous, calls for a legal conclusion. 14:12:03

THE WITNESS: My memory is such, I recall 14:12:06
papers that were referred to in the patent 14:12:08
specification. But as to whether I'm leveraging those 14:12:12
specific references in my statement of enablement, I 14:12:16
don't recall. I mean if you're saying there was a 14:12:19
reference paper in the patent spec and whether I'm 14:12:22
using that reference to make my enablement claim? 14:12:22

BY MS. MOEHLMAN: 14:12:28

Q. Yes.

A. I just don't recall. I don't think so. I was primarily thinking about the particular implementation of the preferred embodiment and asking myself -- I mean that's -- so I'm trying to -- yeah, I was primarily looking at the particular implementation of the preferred embodiment and asking myself if I felt that a -- that a functioning system could be built using that particular preferred embodiment that embodies the claims. And I felt that it could. It may be that there's, you know, parts of that opinion leverage something that's referred in the -- but I just don't have that level of detail to recall it. 14:12:32 14:12:37 14:12:42 14:12:53 14:12:55 14:12:59 14:13:05 14:13:10 14:13:14 14:13:22 14:13:26 14:13:29

Q. Did you review the papers that are incorporated by reference? 14:13:33 14:13:34

A. I only reviewed those papers that were called out in the validity, in the validity charts. So I didn't go through any of the other papers that weren't called out. 14:13:37 14:13:43 14:13:49 14:13:52

Q. So for example, if you take the '615 patent and you look in column 5 -- 14:13:55 14:14:07

A. Yeah, I'm here. 14:14:09

Q. -- okay, and you go to about line 52 -- 14:14:15

A. I've got you. 14:14:17

Q. -- and you'll see there is a reference to a paper by Mr. Valdes and Ms. Anderson. Did you review 14:14:19

that paper? 14:14:25
A. Line 5, 52? 14:14:28
Q. Column 5, line -- yeah, the sentence that 14:14:32
starts on 52. 14:14:34
A. Right. On NIDES. I did look at this paper 14:14:42
some months ago in the context of reading up on NIDES. 14:14:51
Q. Do you believe that the content of that 14:14:53
paper is necessary in order for one of skill in the 14:15:00
art to practice the claims of the patents in suit? 14:15:05
A. No, I don't believe so. 14:15:34
Q. If you could turn to column 12 -- actually, 14:15:50
it's column 13. You'll see that there is a reference 14:15:53
to the Porras and Valdes paper "Live Traffic 14:15:53
Analysis." 14:16:01
A. What line are you on? Oh, right at the top. 14:16:05
Q. Right at the top. 14:16:06
A. Yes. 14:16:06
Q. Do you believe that any material from that 14:16:09
paper is necessary in order to practice -- is 14:16:12
necessary in addition to what is disclosed in the 14:16:14
specification in order to build the claims of the 14:16:20
patents in suit? 14:16:21
A. I would say yes. The "Live Traffic" paper 14:16:30
does disclose -- let me just double -- do you mind if 14:16:38
I just double-check something with regard to "Live

Traffic"? 14:17:25

Sorry. Yeah, I don't change my answer. 14:17:33

Q. I'm sorry -- 14:17:34

A. Sorry, did I answer the question? Sorry, 14:17:36
could you repeat your question? 14:17:37

Q. Is it your testimony that the "Live Traffic 14:17:43
Analysis" paper discloses material not in the patent 14:17:48
specification that is necessary to practice the 14:17:53
claims of the patents in suit? 14:17:55

A. Not in the patent specification? 14:17:56

MR. POLLACK: Objection. Vague and 14:17:57
ambiguous, lacks foundation. 14:18:04

THE WITNESS: I never thought of it that way. 14:18:07
I never thought that the "Live Traffic" paper -- I 14:18:15
mean they're -- it discloses things that are not in 14:18:18
the patent spec. But did you say that are necessary? 14:18:30
Sorry, I hate to have you repeat it again. This is 14:18:34
the third time. 14:18:34

BY MS. MOEHLMAN: 14:18:37

Q. It's okay. Why don't we do it this way. 14:18:41
What does it disclose that's not in the patent 14:18:45
specification? 14:18:46

MR. POLLACK: Objection. Overbroad, vague 14:18:48
and ambiguous, lacks foundation. 14:19:01

THE WITNESS: I think it gets into greater

specific detail on techniques, as the title suggests, 14:19:09
on techniques of traffic analysis. And I'm not even 14:19:23
sure that that's true, that it gets into greater 14:19:25
detail. 14:19:27

I never really looked at it from the 14:19:30
perspective of comparing the "Live Traffic Analysis" 14:19:34
paper to the patent specification per se, so I'm 14:19:37
having a hard time mapping what I know of that paper 14:19:40
to what is disclosed in the spec. And I didn't opine 14:19:52
on it in my report. I was thinking of the "Live 14:19:55
Traffic" paper with regard to the claims rather than 14:19:58
with regard to the spec. 14:20:00

So I guess at this point, I really -- perhaps 14:20:06
I can answer the question tomorrow and just think on 14:20:11
it in between. 14:20:11

BY MS. MOEHLMAN: 14:20:12

Q. Sure. 14:20:17

A. So just to clarify, you're asking what is 14:20:22
disclosed in the "Live Traffic Analysis" paper that 14:20:26
was not disclosed, specifically not disclosed in the 14:20:29
spec? 14:20:29

Q. Right. 14:20:30

A. Okay. 14:20:30

Q. And I'm also asking whether or not there is 14:20:34
material in the "Live Traffic Analysis" paper that is

not disclosed in the patent specification that would 14:20:41
be needed by one of skill in the art to build the 14:20:46
claims of the patents in suit. 14:20:49

A. Not all of them, but -- as I stipulate in my 14:20:53
report. But the majority of them, certainly, I think, 14:21:01
do -- what I'm trying to say is the "Live Traffic 14:21:08
Analysis" paper teaches some of the claims. 14:21:17

I mean I'm just having a hard time, because 14:21:20
the thinking about the "Live Traffic Analysis" paper 14:21:23
in the context of the spec. 14:21:24

But with regard to the claims, you know, 14:21:35
we're contending that if the "Live Traffic Analysis" 14:21:37
paper is considered prior art, that there are 14:21:40
additional claims that it simply doesn't teach. There 14:21:47
are certain claims that it simply doesn't teach. 14:21:52

Q. Let me ask the question in a different way. 14:21:54
Let's assume that there was no reference to the "Live 14:22:02
Traffic Analysis" paper in the patent specification, 14:22:10
and so that you couldn't look at that paper. Without 14:22:15
any -- without that paper, would the claims of the 14:22:21
patents in suit, would one of skill in the art be 14:22:23
able to practice the claims of the patents in suit? 14:22:27

A. I believe so. I believe so. 14:22:58

Q. Going back to Kesidis Exhibit 1, this is an 14:23:02
opinion that you wrote regarding the infringement of

certain ISS products; is that correct? 14:23:08
A. Right. 14:23:14
Q. Now, you -- in your opinion, you talk about 14:23:20
the '203, the '615 and the '338 patent. Is it your 14:23:28
opinion, Dr. Kesidis, that ISS products do not 14:23:32
infringe the claims of the '212 patent? 14:23:38
MR. POLLACK: Objection. Lacks foundation. 14:23:44
THE WITNESS: In truth, I really haven't 14:23:46
given it much thought any time recently. So I'm just 14:23:52
inferring by its absence that we didn't explore that 14:24:08
avenue. 14:24:08
BY MS. MOEHLMAN: 14:24:08
Q. So you don't have an opinion one way or the 14:24:10
other as to whether any ISS product infringe -- 14:24:15
A. '212? 14:24:16
Q. -- infringe the claims of the '212 patent? 14:24:23
A. I just -- I'm just not prepared to answer. I 14:24:26
just don't know. Any ISS products that I read about, 14:24:40
right? I guess I just -- it's not here. It's not 14:24:44
present. So I imagine the answer should be no. But 14:24:46
I'm not sure how I would elaborate on that. 14:24:56
Q. Now, you state in the third paragraph 14:25:07
that -- 14:25:08
A. Sorry, paragraph 3? 14:25:10
Q. Paragraph 3 of Kesidis Exhibit 1, that it is

your opinion: 14:25:15

"That ISS agents, both RealSecure 14:25:19
agents, network guard server and 14:25:22
desktop series and Proventia agents, 14:25:25
(A, G, M, Server and Desktop series), 14:25:28
when used in combination with the 14:25:32
SiteProtector security Fusion module 14:25:36
2.0, as well as later versions, 14:25:38
infringe certain claims of the '615 14:25:41
and the '203 patent." 14:25:43

Correct? 14:25:44

A. Right. 14:25:45

Q. Is it your opinion that ISS agents, when 14:25:51
used in combination with SiteProtector but not with 14:25:57
Fusion, is not infringing? 14:26:01

A. Right. That's my opinion. 14:26:08

Q. So it's your opinion that the Fusion module 14:26:11
2.0 has to be present in order for there to be 14:26:15
infringement, correct? 14:26:16

A. That's correct. 14:26:16

Q. Now, do you understand that Fusion has 14:26:19
different components? 14:26:20

MR. POLLACK: Objection. Vague and 14:26:26
ambiguous. 14:26:26

THE WITNESS: Sure, right.

ambiguous. Lacks foundation. 16:40:32

THE WITNESS: I'm not aware of any deployed, 16:40:34
any hierarchical monitor deployed at that time, circa 16:40:41
January 2003, when Slammer struck that affected 16:40:51
anything to mitigate its spread. That is to say, I've 16:40:57
never read any published accounts of the effectiveness 16:41:00
of one hierarchical monitor or another on the 16:41:08
particular worms I discuss on page 42 of Exhibit 1. 16:41:17

MS. MOEHLMAN: I'd like to mark as Kesidis 16:41:23
Exhibit 12 a document entitled "Architecture Design of 16:41:28
a Scalable Intrusion Detection System for the Emerging 16:41:32
Network Infrastructure," bearing production numbers 16:41:35
ISS 27334 through 374. 16:41:53

(Defendants' Exhibit 12 was marked for 16:41:54
identification.) 16:41:54

MS. MOEHLMAN: Although the production 16:41:57
numbers got cut off at the end. 16:41:57

BY MS. MOEHLMAN: 16:42:22

Q. Do you recognize this as the architecture 16:42:24
design document for JiNao? 16:42:26

A. Yes. 16:42:26

Q. Have you read this document? 16:42:29

A. I did. 16:42:35

Q. I'd like you to turn to figure 1 which is on 16:42:39
page 4. And do you see in the local detection

module, there is a box labeled "statistical analysis" 16:42:52
right? 16:42:53
A. Right, I see that, question. 16:42:56
Q. Do you understand that the statistical 16:42:58
analysis was adopted from the NIDES work? 16:43:00
MR. POLLACK: Objection. Vague and 16:43:04
ambiguous. 16:43:04
THE WITNESS: I understand that's what it 16:43:07
says, yes. 16:43:07
MS. MOEHLMAN: 16:43:07
Q. Okay. And do you see at the bottom, there 16:43:13
is a circle that says "Network"? 16:43:16
A. I see that. 16:43:17
Q. And it goes to an interception module, and 16:43:21
then it goes into the JiNao agent. Do you see that? 16:43:26
A. Yes, I see that, yes. 16:43:28
Q. Does that indicate to you that JiNao is 16:43:35
receiving network packets? 16:43:36
MR. POLLACK: Objection. Vague and 16:43:37
ambiguous. 16:43:41
THE WITNESS: I'm a little bit lost. Maybe 16:43:46
the figure is not right. The network seems to be 16:43:55
inputting into something called an "interception 16:43:58
module." And I believe the arrow from the 16:44:03
interception module should go into the -- sorry.

BY MS. MOEHLMAN: 16:44:13

Q. Should go into the prevention module? 16:44:20

A. I'm -- I didn't look at this figure too 16:44:23
carefully. Now I'm not sure I understand it. I think 16:44:29
maybe the arrow direction on the interception module 16:44:33
should be reversed. 16:44:38

Q. I think it's not the best copy. I believe 16:44:40
it's -- 16:44:41

A. Or is it a double arrow? 16:44:44

Q. Yeah. I believe it is? 16:44:45

A. That's what I thought. I thought it must be. 16:44:48
Okay. I just take your word for it that it's a double 16:44:54
arrow. 16:45:17

Q. Okay. So does that indicate -- oh, so just 16:45:21
to show you a better version of the picture so you 16:45:28
can confirm for yourself -- 16:45:29

A. That's fine. 16:45:30

Q. -- that's a double arrow. 16:45:33

A. I see it. It had to be. 16:45:34

Q. Okay. So does that show in this figure that 16:45:39
the JiNao monitor receives packets from the network 16:45:42
through the interception module? 16:45:46

MR. POLLACK: Objection. Vague and 16:45:48
ambiguous, lacks foundation. 16:45:52

THE WITNESS: Based on this figure, it

receives certain packets from the network. 16:45:53

BY MS. MOEHLMAN: 16:46:01

Q. Now, if you turn to the next page, it goes through -- the packets go through something called the prevention module. And if you look on page 5, prevention module, it says: 16:46:04 16:46:07 16:46:14 16:46:15

> As the name "prevention" implies, this module will implement a small set of administrative rules to filter out any packet with clear security violations before it enters into the router." 16:46:18 16:46:21 16:46:23 16:46:25 16:46:26 16:46:27

Do you see that? 16:46:28

A. Yes. 16:46:29

Q. And then it may discard some packets, but then it may allow some packets through; is that correct? 16:46:42 16:46:42 16:46:46

A. I see that, correct. 16:46:47

Q. And then it goes through the detection module, correct? 16:46:49 16:46:49

A. (Nods head up and down.) 16:46:50

Q. So the statistical analysis and the protocol analysis are performed on network packets, correct? 16:46:52 16:46:57

MR. POLLACK: Objection. Lacks foundation, assumes facts. 16:47:01

THE WITNESS: Sorry, can you repeat that last question? 16:47:03 16:47:03

BY MS. MOEHLMAN: 16:47:04

Q. As indicated by figure 1, the JiNao architecture at the local detection module would analyze network packets, correct? 16:47:10 16:47:14 16:47:16

A. Right. 16:47:17

MR. POLLACK: Same objection. 16:47:17

BY MS. MOEHLMAN: 16:47:19

Q. Now, if you look on this figure at the JiNao system architecture, do you see there's two boxes at the top, and they are -- they have a box saying "Management Interface"? Do you see that? The small boxes that are on the left side. 16:47:23 16:47:28 16:47:36 16:47:46 16:47:47

A. Oh", Management Interface," yes. 16:47:50

Q. And in those boxes, you see two other boxes. One is statistical analysis, and one is protocol analysis. Do you see that? 16:47:53 16:47:57 16:47:58

A. I see that. 16:47:58

Q. And those are the same labels for those boxes as indicated in the local detection module of the monitor that's blown out, correct? 16:48:02 16:48:07 16:48:09

MR. POLLACK: Objection. Document speaks for itself. 16:48:11 16:48:11

THE WITNESS: Right.

BY MS. MOEHLMAN: 16:48:12
Q. Do you have any reason to believe that the 16:48:19
statistical analysis at the manager level would be 16:48:26
different than the statistical analysis algorithm 16:48:29
suggested for the local detection module? 16:48:32
MR. POLLACK: Objection. Lacks foundation, 16:48:34
assumes facts. 16:48:35
THE WITNESS: At the local detection module? 16:48:35
BY MS. MOEHLMAN: 16:48:41
Q. Mm-hmm. 16:48:44
A. My recollection of the management agent, 16:48:51
which -- is that the analysis performed there is 16:48:56
essentially on -- I believe is on the MIB itself, 16:49:06
whereas I believe that the local detection module is 16:49:11
looking at, in the case of JiNao, looking at 16:49:20
router-related packets directed at this particular 16:49:22
line card on the fly. 16:49:32
It's trying to do an anomaly detection, but 16:49:42
I -- let me just take a look at -- I'm just trying to 16:50:20
recall specifically the kinds of anomalous signatures 16:50:24
or, sorry, statistically anomalous behavior JiNao is 16:50:31
trying to do locally. I just -- I don't recall 16:50:42
reading a lot about what happened, what kind of 16:50:47
statistical analysis JiNao advocates on the MIB. 16:50:55
Let me just take a quick parse through this